This article was downloaded by: [Nanyang Technological University]
On: 26 August 2015, At: 00:24
Publisher: Taylor & Francis
Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: 5 Howick Place, London, SW1P 1WG

Journal of Discrete Mathematical Sciences and Cryptography
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tdmc20

DNA cryptography: a novel paradigm for secure routing in Mobile Ad hoc Networks (MANETs)

A. K. Verma [a] , Mayank Dave [b] & R. C. Joshi [c]

[a] Department of Computer Science and Engineering , Thapar Institute of Engineering & Technology (Deemed University) , Patiala , India

[b] Department of Computer Engineering , National Institute of Technology , Kurukshetra , India

[c] Department of Electronics and Computer Science , Indian Institute of Technology , Roorkee , India

Published online: 03 Jun 2013.

To cite this article: A. K. Verma , Mayank Dave & R. C. Joshi (2008) DNA cryptography: a novel paradigm for secure routing in Mobile Ad hoc Networks (MANETs), Journal of Discrete Mathematical Sciences and Cryptography, 11:4, 393-404, DOI: 10.1080/09720529.2008.10698192

To link to this article: http://dx.doi.org/10.1080/09720529.2008.10698192

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at http://www.tandfonline.com/page/terms-and-conditions

DNA cryptography: a novel paradigm for secure routing in Mobile Ad hoc Networks (MANETs)

A. K. Verma *

Department of Computer Science and Engineering
Thapar Institute of Engineering & Technology (Deemed University)
Patiala
India

Mayank Dave †

Department of Computer Engineering
National Institute of Technology
Kurukshetra
India

R. C. Joshi ‡

Department of Electronics and Computer Science
Indian Institute of Technology
Roorkee
India

Abstract

Ad hoc networks do not necessarily rely on fixed infrastructure for the communication amongst its various nodes and this poses new challenges for the necessary architecture they apply. In addition, ad hoc networks are often designed for specific environments and may have to operate with full availability in difficult situations making them vulnerable as compared to traditional networks. In this paper, we propose a novel secure ad hoc routing protocol that uses pseudo DNA cryptography. The presented work deals with the assumptions, length analysis and evaluation of pseudo DNA algorithm, which can be implemented for securing Ad hoc Networks.

Keywords : *Ad hoc networks, DNA Cryptography, security.*

E-mail: akv_1001@yahoo.com

†*E-mail*: mayank@computer.org

‡*E-mail*: joshifcc@iitr.ernet.in

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 11 (2008), No. 4, pp. 393–404
© Taru Publications

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

1. Introduction

Mobile Ad hoc networks (MANETs) are a type of wireless networks, offering unrestricted mobility without any underlying infrastructure. Basically, ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network. Each node in a MANET acts as a host and a router. MANETs have found their application in providing extremely flexible method of establishing communications in situations where, geographical constraints demand a totally distributed network system, without any fixed base station such as, military operations, battle fields, remote areas etc. Dynamic topologies, bandwidth constraint operation, limited resources and decentralized control characterize these networks.

DNA cryptography [1,2] is a new and very promising direction in cryptography research. DNA can be used in cryptography for storing and transmitting the information, as well as for computations. Although in its primitive stage, DNA cryptography is very effective. Currently, several DNA computing algorithms are proposed for — cryptography, cryptanalysis and steganography problems.

The rest of the paper deals with, starting from importance of securing ad hoc networks followed by an extensive discussion on DNA pseudo Cryptography techniques. In Section 4, we highlight various concerns related to security in ad hoc networks. Section 5 describes the analysis and evaluation of proposed pseudo DNA cryptography algorithm and finally we conclude with the future scope.

2. Motivation

Ad hoc networks are highly vulnerable to security attacks and dealing with this is one of the main challenges of developers of these networks today. The main reasons are [3] — Shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among nodes, limited availability of resources, and physical vulnerability. Generally, when considering the security of a network, we analyze the network against the following parameters:

- *Availability* refers to the fact that the network must remain operational at all times despite denial of service (DoS) attacks [4].

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

- *Confidentiality* ensures that certain information is never disclosed to certain users. Authentication is the ability of a node to identify the node with which it is communicating.
- *Integrity* guarantees that a message is never corrupted when transferred.
- *Non-repudiation* states that the sender of the message cannot deny having sent it.

Whereas, an ad hoc network has extra security requirements caused by its lack of proper infrastructure and the dynamic relationship between the nodes in the network. The accountability is very difficult to determine as there is no central authority, which can be referenced when it comes to making trust decisions about other parties in the network.

The dynamic relationship between the nodes leaves very little opportunity for the nodes to form trust relationships [5] with each other. In an ad hoc network, nodes must act as both terminals and routers for other nodes. There are no dedicated nodes; therefore, a secure routing protocol [6] is needed. Further, the multi-hop routing protocols usually lead to problems like non-cooperating nodes and denial of service (DoS) attacks. Researchers in the past have proposed secure routing protocols [11], which are compared in Table 1.

Table 1
Comparison of secure routing protocols for MANETs

Performance → / Parameters ↓	ARAN	ARIADNE	SAODV	SAR	SEAD	SLSP	SRP
Type	Reactive	Reactive	Reactive	Reactive	Proactive	Proactive	Reactive
MANET protocol	AODV/ DSR	DSR	AODV	AODV	DSDV	ZHLS	DSR/ ZRP
Encryption	Asym	Sym	Asym	Sym/ Asym	Sym	Asym	Sym
Synchronization	No	Yes	No	No	Yes	No	No
Trust authority	CA	KDC	CA	CA/ KDC	CA	CA/ KDC	CA
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Confidentiality	Yes	No	No	Yes	No	No	No
Integrity	Yes	Yes	Yes	Yes	No	No	Yes
Non-repudiation	Yes	No	Yes	Yes	No	Yes	No
Anti-spoofing	Yes	Yes	Yes	Yes	No	Yes	Yes
DoS attacks	No	Yes	No	No	Yes	Yes	Yes

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

As can be observed, none of the algorithm defends against all possible type of attacks. We hereby propose a novel scheme to secure Ad hoc Networks using Pseudo DNA cryptography.

3. Pseudo DNA cryptography

The central dogma of the molecular biology is illustrated in the following Figure 1.

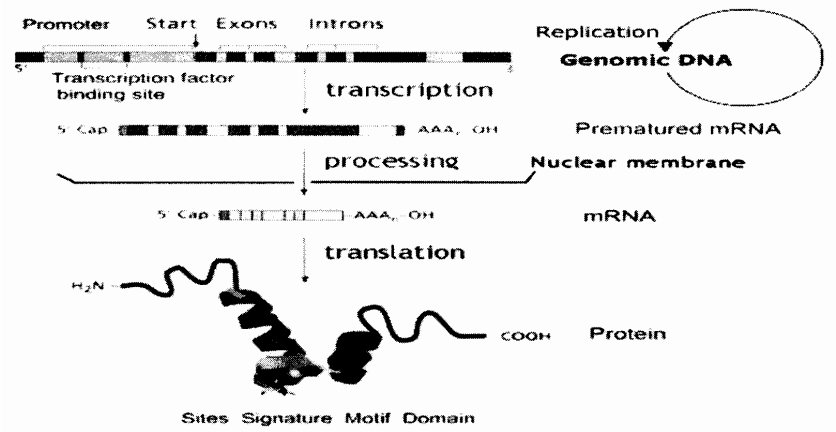

Figure 1

The *Central Dogma* of molecular biology [12]

The transcription, splicing and translation processes are briefly explained below:

Transcription and splicing. A DNA segment consisting of a gene is read, starting from the promoter, which is the starting position of the DNA segment. Then the non-coding areas (intron) are removed according to certain tags, leaving behind the coding areas (extron) that are rejoined and caped. The sequences in transcribed in to a single stranded sequence of mRNA (messenger RNA). The mRNA moves from the nucleus into the cytoplasm.

Translation. As the protein is formed, the mRNA sequence is translated into a sequence of amino acids. The ribosome read the fragment starting from certain three-bases during translation. The ribosome read s three bases (a codon) at a time from the mRNA and translates them into one amino acid. To sign the end of translation, we have certain ending three-bases.

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

In a nutshell, the introns are cut out, and extrons are kept to from mRNA, which will perform the translation work during the first step (Transcription and Splicing) and then during translation, the codons are translated into the amino acids according to the genetic code table [13].

3.2 *Method*

The proposed pseudo DNA cryptography method is similar to the two basic steps as explained above. In order to make the cryptographic process more secure, some changes are desired in the splicing process i.e. the start codes and pattern codes specify the introns to be deployed and further the pattern codes are non- continuous. Thus making it difficult to guess on introns as they are now spaced.

3.3 *Adaptability*

The information is stored in the binary form and can be transformed into DNA form representing four different bases Adenine, Guanine, Thiamine, and Cytosine using 2-bit code for each of them.

Now, the sender also knows the starting codes (beginning of intron) and pattern codes (defining which part to be removed), so the following steps are followed:

(i) DNA form of information is scanned by the sender to find out the introns recording the information about: introns places and cut out introns. So, the DNA form of data is translated into mRNA form of data.

(ii) The sender translates this mRNA data into protein form of data based upon the genetic code table.

(iii) Before transmitting over a secure channel to the receiver, the starting and pattern codes of the introns, the places of the introns the removed spaced introns and the codon-amino acids mapping of the protein are keys used to decrypt the protein form of data.

(iv) When the receiver gets these keys through the secure channel from the sender (or Public Key Protocol can be used). On receiving the protein form of data, the receiver uses the keys to recover mRNA and then DNA form of information. This method is illustrated in Figure 2.

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

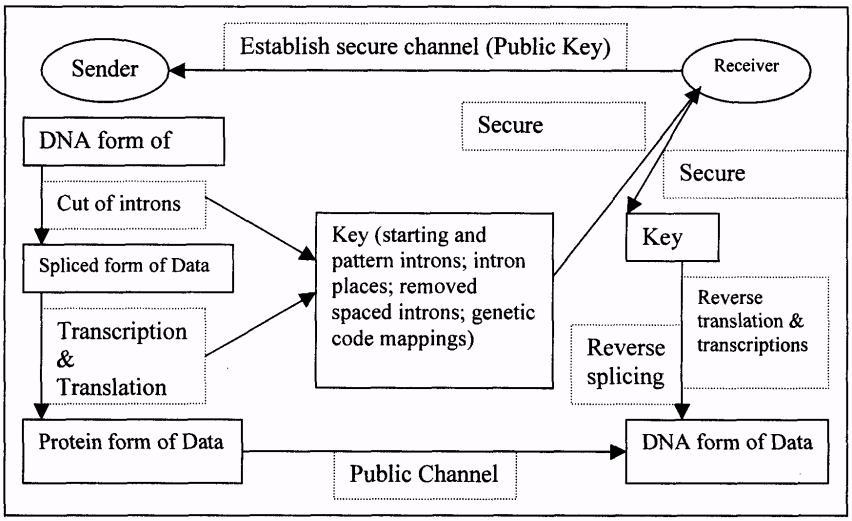

Figure 2

The implementation diagram of the pseudo DNA cryptography method

In general, this scheme is formulated as below (M and C are for plaintext and cipher text, respectively):

- Encryption key EI = (the starting and pattern codes of the introns, the places of the introns)
- Encryption key $E2$ = (the codon-amino acids mapping)
- Decryption key $D_1 = E_2$
- Decryption key $D_2 = E_1$
- $C' = E_1(M), C = E_2(C')$
- $M' = D_1(C), M = D_2(M')$

As observed, the proposed scheme is principally a symmetric key algorithm, except that the sender initially has only a part of the keys, and he generates the rest part of the keys.

4. Routing security in Ad hoc Networks

The attackers can be divided into two classes, *active* and *passive*. An active attacker injects packets into the networks and also eavesdrops, whereas a *passive* attacker does not send messages; it only eavesdrops

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

on the network. Such attackers are threat to the privacy or anonymity of communication, rather than the routing protocol.

The attacks on routing protocols can also be divided into two categories: *routing disruption* and *resource consumption*.

In routing disruption attacks, the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways. For example, Denial of Service (DoS) Attack [4], Routing Loop [7], Black hole [8], Gray Hole [8], Gratuitous Detour [10], Blackmail Attack [10], Wormhole Attack [7], Rushing Attack [9].

In *Resource Consumption Attack*, the attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth, or to consume node resources such as memory (storage) or computation power. Denial of Service Attack can also be counted as an instance of *Resource Consumption Attack*. Another example is to inject extra data packets and extra control packets to consume the network resources.

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

5. Algorithm analysis and evaluation

5.1 *Analysis of pseudo DNA cryptography*

Let us suppose that the DNA form of information D has a length n. There are k introns, and their average length is m. Then the mRNA form of information D' have the length $n - k * m$. Since one codon (consists of 3 nucleic acids) generally can be translated into one amino acid, the protein form of information D'' have the length of $(n - k * m)/3$. Both the encryption and decryption process have the time complexity of $O(n)$.

As there are 61 coding Codons, and only 20 amino acids, thus on an average 3 codons to be mapped on to the same amino acid, so the different number of mRNA for the protein form of data is about $3^{(n-k*m)/3}$ In reverse transcription process there are $2^{(n-k*m)}$ places to insert introns. Now, even if the introns are known, the time complexity of recovering DNA form data from mRNA form is $O(k * 2^{(n-k*m)})$. If spaced intron scheme is used, the time complexity can be $0(2^k \times 2(n^{(n-k*m)})$. So the total time complexity can be at least $0(3(n - k * m) \times 2^{(n-k*m)})$. Further by careful control, if $k * m$ is around $0.35n$ $(= \log_2 3/(\log_2 3 + 3) * n)$, then the complexity above is $O(2^n)$. The smaller the $k * m$, such time complexity can be increased, but more partial information would be revealed, which makes it venerable to other attacks. Since n is generally of the 1Mb scale, such a brute force attack method is unpractical.

However, if an attacker is given enough plaintexts and computation, the method is not so strong against chosen plaintext attacks because knowing the mechanisms of the method there is a high probability that the attacker can get partial or full knowledge about the keys with high probability.

5.2 *Evaluation*

The encryption/decryption algorithm has been performed in C-language under Linux system. Each of the encryption/decryption process is performed ten times and the average time is considered and for checking the robustness of the system, we have selected four different plain texts with increasing size.

The program is designed for a simple sender-receiver system. On the sender side, an initial key is required (starting introns and pattern codes) which the user himself generates. The user first translates the plaintext into DNA form of information using conversion program. Processes of central dogma — splicing, transcription and translation are also simulated including necessary padding for compatibility reason. Now, the starting and pattern codes of the introns along with the places of introns, removed spaced introns and the codon-amino acid are added into the key file and the enciphered information is also created. These two files are then sent to receiver through two different channels, the enciphered file through public channel and the key file through secure channel.

At the receiver side, the enciphered information and the key file are received from two different channels. The key information in the key file is used to decipher the received information. Reverse translation, reverse transcription and reverse splicing processes are applied using the respective program and the information stored in the key file. After this process the receiver gets the DNA form of information and then the plain text can be easily recovered in order to know what the sender has sent to the receiver.

We have used highly divert plaintext, which include short-text, long-text purely alphabetical and text combining alphabets in order to test the performance of the program. The following Table 2 shows the different texts considered:

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

Table 2

Performance of application with plaintext of different contents

Dataset	Description	Number of different characters	Recovery of plaintext
Test1	Only alphabetical and digital characters	52	Yes
Test2	Only non-alphabetical and non-digital characters	100	Yes
Test3	Combination of characters	75	Yes
Test4	Combination of characters	125	Yes

Further, each plaintext has the length 10 times that of the former one, starting from 10 and then number bits needed to store in ASCII format is calculated, which is eight times the length of plain text. As observed

For cipher text, the length and the relative bits are also calculated. Since, one amino acid can be represented by a 3-letter sequence, and for unique 64 amino acids, we require 6 bits and only 2 bits are needed for each letter in cipher text.

As a result, the number of bits needed for each of cipher-text is double the length of cipher text. We have also introduced the redundancies (tags and separators). The actual key information is dependent on size of the starting and pattern codes of the introns but its size is roughly less than half of the size including redundancy (Table 3). The encryption and decryption times are also listed, which points towards the efficiency of the algorithm (Figure 4).

Table 3

Performance of the application with plaintexts of different lengths

Dataset	Length of plaintext time (Bits)	Length of cipher text (Bits)	Size of key (with redundancy)	Encryption time (ms)	Decryption time (ms)
Test1	10 (80)	51 (102)	100	254	428
Test2	100 (800)	396 (792)	708	258	431
Test3	1000 (8000)	3521 (7042)	5211	298	483
Test4	10000 (80000)	36212 (72424)	48132	1292	1398

6. Conclusion and future work

We have proposed a pseudo DNA cryptography method, a cryptography method based on central dogma of molecular biology. The method simulates the transcription and translation process of the central

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

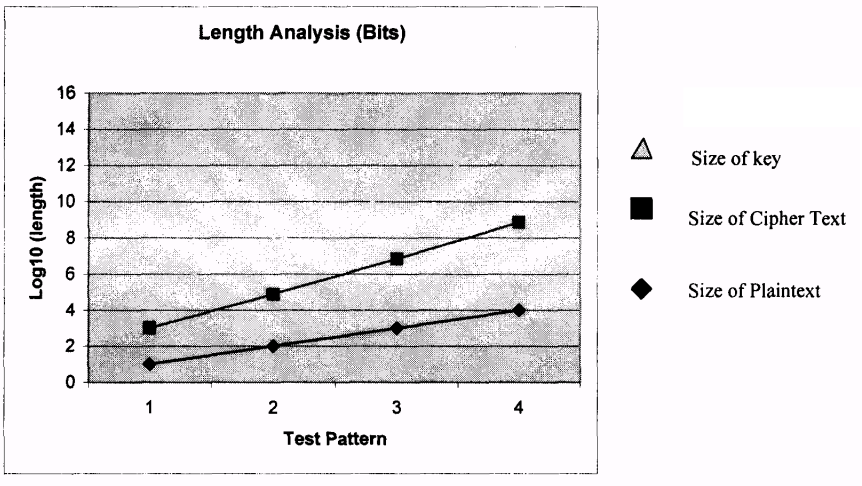

Figure 3
Analysis of Length of plaintext and cipher text

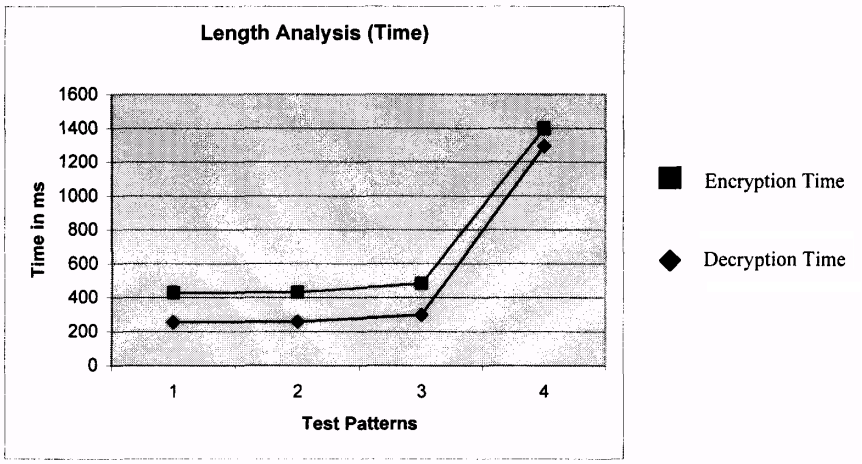

Figure 4
Analysis of time for encryption and decryption time

dogma; it also adds some artificial features to make the resulting cipher texts difficult to break. The theoretical analysis shows that this method is powerful against certain attacks, especially against brute force attacks. The experiments not only show the power of such a method, but also reveal that this method is very efficient in computation as well as very robust.

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

To provide more complexity, the codon-amino acids mapping can be modified artificially in order to thwart brute force attacks. However, this method has its share of shortcomings too. There is some existence of partial information which enables the attacker to infer the whole information by using small amount of effort and further, the a confusion of the plaintext is not very complete, although the later can be overcome by having multiple rounds of encryption on plain text to achieve ciphertext or we can use a more flexible splicing rule.

References

[1] A. Gehani, T. LaBean and J. Reif, DNA-based cryptography, *DIMACS DNA Based Computers V*, American Mathematical Society, 2000.

[2] D. Nixon, *DNA and DNA Computing in Security Practices – Is the Future in Our Genes?*, GSEC Assignment Version 1.3.

[3] N. Asokan and P. Ginzboorg, Key management in ad hoc networks, *Computer Communications*, Vol. 23 (2000), pp. 1627–1637.

[4] D. B. Faria and D. R. Cheriton, DoS and authentication in wireless public access networks, in *Proceedings of the First ACM Workshop on Wireless Security* (WiSe'02), September 2002.

[5] B. K. R. Yahalom and T. Beth, Trust relationships in secure systems – a distributed authentication perspective, *Computer System*, Vol. 7 (1) (1994), pp. 45–73.

[6] M. G. Zapata and N. Asokan, Securing ad hoc routing protocols, in *Proceedings of the ACM Workshop on Wireless Security* (WiSe 2002), September 2002.

[7] Y. C. Hu, A. Perrig and D. B. Johnson, Wormhole detection in wireless ad hoc networks, Department of Computer Science, Rice University, *Tech. Rep. TR01-384*, June 2002.

[8] C. Adjih, T. Clausen, A. Laouiti, P. Mühlethaler and D. Raffo, Securing the OLSR routing protocol with or without compromised nodes in the network, *Technical Report INRIA RR-5494, HIPERCOM project*, INRIA Rocquencourt, February 2005.

[9] Y. C. Hu, A. Perrig and D. B. Johnson, Rushing attacks and defense in wireless ad hoc network routing protocols, in *Proc. ACM Workshop on Wireless Security*, 2003.

[10] P. Papadimitratos and Z. Haas, Secure routing for mobile ad hoc networks, in *Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference* (CNDS), 2002.

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015

[11] A. A. Prizada and C. McDonald, Secure routing protocols for mobile ad hoc wireless networks, in *2nd Workshop on Internet, Telecommunication and Signal Processing*, WITSP 2003, Australia, pp. 57–80, 2003.

[12] L. Adleman, Molecular computation of solutions to combinatorial problems, *Science*, Vol. 266 (November 1994), pp. 1021–1024.

[13] M. Yarus, RNA-ligand chemistry: a testable source for the genetic code, *RNA*, Vol. 6 (2000), pp. 475–487.

Received December, 2006

Downloaded by [Nanyang Technological University] at 00:24 26 August 2015